EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	((authenticat$3 near5 (client or user)) and (compar$3 with (first adj3 certificate) with ((second or another) adj3 certificate))).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:10
L2	2	((authenticat$3 near5 (network adj5 device)) and (compar$3 with (first adj3 certificate) with ((second or another) adj3 certificate))).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:14
L3	0	((authenticat$3 near5 (network adj5 device)) and (compar$3 with (other adj3 certificate) with (stored adj3 certificate))).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:15
L4	0	((authenticat$3 near5 (network adj5 device)) same (compar$3 with (other adj3 certificate) with (stored adj3 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:16
L5	0	((authenticat$3 near5 (network adj5 device)) same (compar$3 with (another adj3 certificate) with (stored adj3 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:17
L6	0	((authenticat$3 near5 (client or user)) same (compar$3 with (another adj3 certificate) with (stored adj3 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:17
L7	0	((authenticat$3 near5 (client or user)) and (compar$3 with (another adj3 certificate) with (stored adj3 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:18
L8	170	((authenticat$3 near5 (client or user)) and (compar$3 with certificate with ((another or second or stored) near5 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:19
L9	52	((authenticat$3 near5 (client or user)) same (compar$3 with certificate with ((another or second or stored) near5 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:45

L10	0	((authenticat$3 near5 (network adj5 device)) same (compar$3 with certificate with ((another or second or stored) near5 certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:45
L11	6	"6145079".pn. or "5903882".pn. or "6957199".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:47
L12	2	infrastructureless with certificate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/08 19:51

Sign in

Google

"infrastructureless certificate"	Search	Advanced Search
		Preferences

Web   Results **1** - **2** of **2** for **"infrastructureless certificate"**. **(0.11** seconds)

Tip: Try removing quotes from your search to get more results.

Method and system for authentication using infrastructureless ...

[0025] Briefly stated, the present invention is directed towards a method and system for authenticating a client employing an **infrastructureless certificate** ...
www.freepatentsonline.com/20050149723.html - 52k - Cached - Similar pages

Method and system for authentication using infrastructureless ...

... present invention relates generally to computer security, and more particularly, to authenticating a client employing an **infrastructureless certificate**. ...
www.freshpatents.com/Method-and-system-for-authentication-using-**infrastructureless-
certificate**s-dt2005070... - 28k - Supplemental Result - Cached - Similar pages

---

"infrastructureless certificate"	Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

P🜨RTAL

Subscribe (Full Service)   Register (Limited Service, Free)   Login

Search: ⦿ The ACM Digital Library   ○ The Guide

+infrastructureless +certificate   SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **infrastructureless** **certificate**   Found **9** of **203,282**

Sort results by	relevance ▾		Save results to a Binder	Try an Advanced Search
Display results	expanded form ▾		Search Tips	Try this search in The ACM Guide

☐ Open results in a new window

Results 1 - 9 of 9

Relevance scale ☐ ▭ ▬ ◼ ◼

1 Authentication: An approach to certificate path discovery in mobile Ad Hoc networks   ◼

He Huang, Shyhtsun Felix Wu

October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**

Publisher: ACM Press

Full text available: 📄 pdf(146.93 KB)   Additional Information: full citation, abstract, references, citings, index terms

Public key certificates prove validity and authenticity of their ownership and possibly other properties. Certificate path discovery is the critical process for public key verification in hierarchical public key infrastructure (PKI) diagrams. This process is conventionally done in centralized public key management system such as central CA or directory. However, in an infrastructure-less environment, such as a mobile ad hoc network, no such central service is present due to network dynamics. Tha ...

Keywords: MANET, certificate path discovery, public key infrastructure, security

2 URSA: ubiquitous and robust access control for mobile ad hoc networks   ◼

Haiyun Luo, Jiejun Kong, Petros Zerfos, Songwu Lu, Lixia Zhang

December 2004 **IEEE/ACM Transactions on Networking (TON)**, Volume 12 Issue 6

Publisher: IEEE Press

Full text available: 📄 pdf(836.70 KB)   Additional Information: full citation, abstract, references, citings, index terms, review

Restricting network access of routing and packet forwarding to well-behaving nodes and denying access from misbehaving nodes are critical for the proper functioning of a mobile ad-hoc network where cooperation among all networking nodes is usually assumed. However, the lack of a network infrastructure, the dynamics of the network topology and node membership, and the potential attacks from inside the network by malicious and/or noncooperative selfish nodes make the conventional network access co ...

Keywords: mobile ad hoc networks, self-organized access control

3 Upper layer issues: Application protocol design considerations for a mobile internet   ◼

Jörg Ott

December 2006 **Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture MobiArch '06**

Publisher: ACM Press

Full text available: 📄 pdf(318.15 KB)   Additional Information: full citation, abstract, references

The Internet protocols were designed for a primarily "fixed" and relatively static network

environment where communication links are stable and exhibit fairly uniform communication characteristics. Mobile wireless communication has fundamentally invalidated some of these assumptions, for (heterogeneous) wireless access networks and even more so for mobile ad-hoc networks (MA-NETs) formed between mobile users: from highly variable link characteristics to temporary disconnections to non-existing e ...

4 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(2.50 MB)   Additional Information: full citation, references, citings

5 Towards designing a trusted routing solution in mobile ad hoc networks

Tirthankar Ghosh, Niki Pissinou, Kami Makki

December 2005 **Mobile Networks and Applications**, Volume 10 Issue 6

Publisher: Kluwer Academic Publishers

Full text available: pdf(1.04 MB)   Additional Information: full citation, abstract, references, index terms

Designing a trusted and secure routing solution in an untrustworthy scenario is always a challenging problem. Lack of physical security and low trust levels among nodes in an ad hoc network demands a secure end-to-end route free of any malicious entity. This is particularly challenging when malicious nodes collude with one another to disrupt the network operation. In this paper we have designed a secure routing solution to find an end-to-end route free of malicious nodes with collaborative effor ...

Keywords: collaborative trust-based routing, colluding malicious nodes, mobile ad hoc networks, secure communication

6 Assessing vulnerabilities: Modeling Ad-hoc rushing attack in a negligibility-based security framework

Jiejun Kong, Xiaoyan Hong, Mario Gerla

September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**

Publisher: ACM Press

Full text available: pdf(186.50 KB)   Additional Information: full citation, abstract, references, index terms

In this paper, we propose a formal notion of network security for ad hoc networks. We adopt a probabilistic security framework, that is, security is defined by a polynomially bounded adversary model, the cost of attack and the cost of defense. In a complex and probabilistic system, we speak of the "infeasibility" of breaking the security system rather than the "impossibility" of breaking the same system. Security is defined on the concept of "negligible", which is asymptotically sub-polynomial w ...

Keywords: asymptotic invariant, neg-ligibility, randomized network algorithms, randomized turing machine, scalability, sub-polynomial

7 Routing 1: A secure ad-hoc routing approach using localized self-healing communities

Jiejun Kong, Xiaoyang Hong, Yunjung Yi, Joon-Sang Park, Jun Liu, Mario Gerla

May 2005 **Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing MobiHoc '05**

Publisher: ACM Press

Full text available: pdf(222.15 KB)   Additional Information: full citation, abstract, references, citings, index terms

Mobile ad hoc networks (MANETs) are vulnerable to routing attacks, especially attacks launched by non-cooperative (selfish or compromised) network members and appear to

be protocol compliant. For instance, since packet loss is common in mobile wireless networks, the adversary can exploit this fact by hiding its malicious intents using compliant packet losses that appear to be caused by environmental reasons.In this paper we study two routing attacks that use non-cooperative network members and d ...

Keywords: community-based security, self-healing ad hoc routing

8 Security: The feasibility of launching and detecting jamming attacks in wireless networks
Wenyuan Xu, Wade Trappe, Yanyong Zhang, Timothy Wood
May 2005 **Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing MobiHoc '05**
Publisher: ACM Press

Full text available: ⬛ pdf(395.70 KB)   Additional Information: full citation, abstract, references, citings, index terms

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. In this paper, we examine radio interference attacks from both sides of the issue: ...

Keywords: denial of service, jammer detection, jamming

9 Wireless monitoring and denial of service: Channel surfing and spatial retreats: defenses against wireless denial of service
Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang
October 2004 **Proceedings of the 2004 ACM workshop on Wireless security WiSe '04**
Publisher: ACM Press

Full text available: ⬛ pdf(327.10 KB)   Additional Information: full citation, abstract, references, citings, index terms

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch denial of service (DoS) attacks. One form of denial of service is targeted at preventing sources from communicating. These attacks can be easily accomplished by an adversary by either bypassing MAC-layer protocols, or emitting a radio signal targeted at jamming a particular channel. In this paper we present two strategies that may be employed by wireless devices to evade a MAC/PHY-layer jamming-style wi ...

Keywords: CSMA, Jamming, denial of service

Results 1 - 9 of 9